Version 0.11

DRAFT – WORK IN PROGRESS

New Concept of Operations
for DoS Open Net and Class Net
Certification and Accreditation

Continuous
Certification and Accreditation

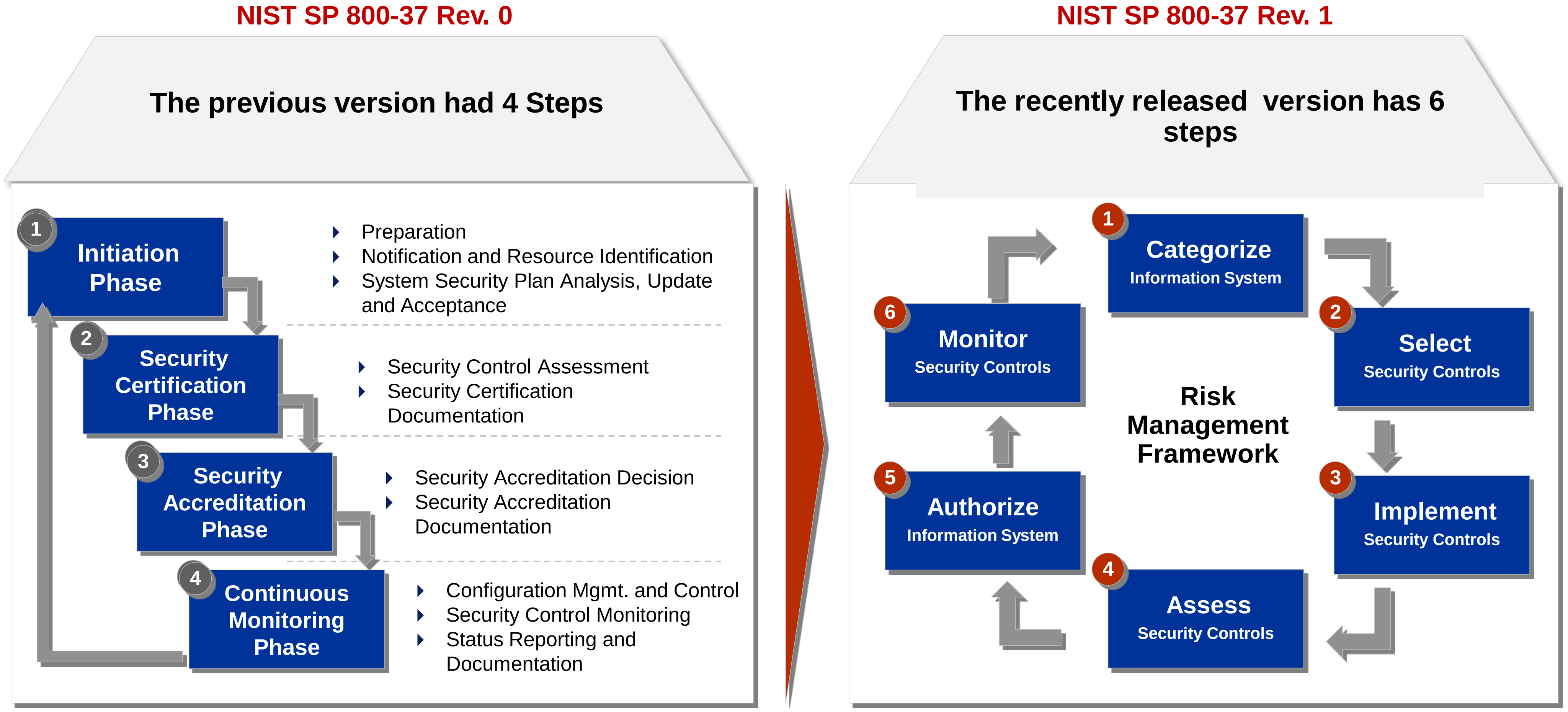
February 2010

This document is sensitive but unclassified (SBU) and is intended solely for the use and information to whom it is addressed.

How can the Department of State leverage its successful Risk Scoring Program?

- **…to improve the OpenNet & ClassNet C&A process?**
- **…to measurably increase security without increasing costs?**

NIST SP 800-37 defines how Federal C&A is to be accomplished



NIST SP 800-37 Rev. 0

The previous version had 4 Steps

1 **Initiation Phase**

- Preparation
- Notification and Resource Identification
- System Security Plan Analysis, Update and Acceptance

2 **Security Certification Phase**

- Security Control Assessment
- Security Certification Documentation

3 **Security Accreditation Phase**

- Security Accreditation Decision
- Security Accreditation Documentation

4 **Continuous Monitoring Phase**

- Configuration Mgmt. and Control
- Security Control Monitoring
- Status Reporting and Documentation

NIST SP 800-37 Rev. 1

The recently released version has 6 steps

Risk Management Framework

1 **Categorize** Information System

2 **Select** Security Controls

3 **Implement** Security Controls

4 **Assess** Security Controls

5 **Authorize** Information System

6 **Monitor** Security Controls

# *= NIST 800-37 Rev. 1 Steps*

# *= NIST 800-37 Rev. 0 Mapping to Rev. 1 Steps*

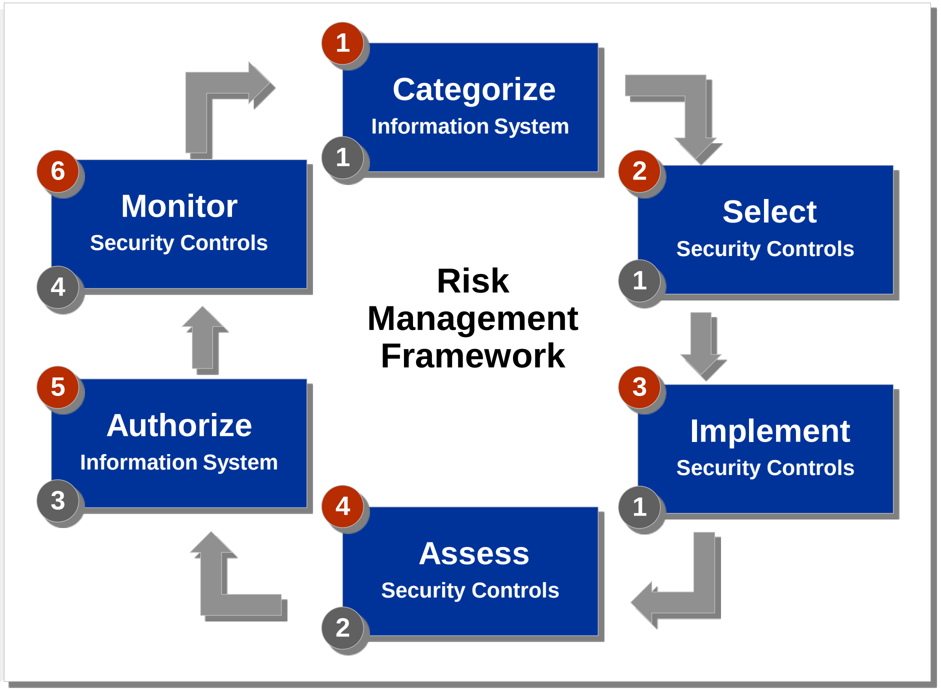
NIST's model is notionally linear yet flexible in its application

Implications

- **The Risk Management Framework when implemented as depicted can take quarters and years to complete, not hours or days.**
- **Federal agencies can improve security by exercising SP800-37 Rev 1's built-in flexibility to:**
  - Guide day-to-day Remediation Decisions
  - Trigger reconsideration of accreditation day-to-day when risk levels exceed pre-defined triggers.

  "***Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF including authorization-related activities."*** **SP800-37 Rev 1**

NIST SP 800-37 Rev. 1



1 Categorize Information System 1
2 Select Security Controls 1
3 Implement Security Controls 1
4 Assess Security Controls 2
5 Authorize Information System 3
6 Monitor Security Controls 4
Risk Management Framework

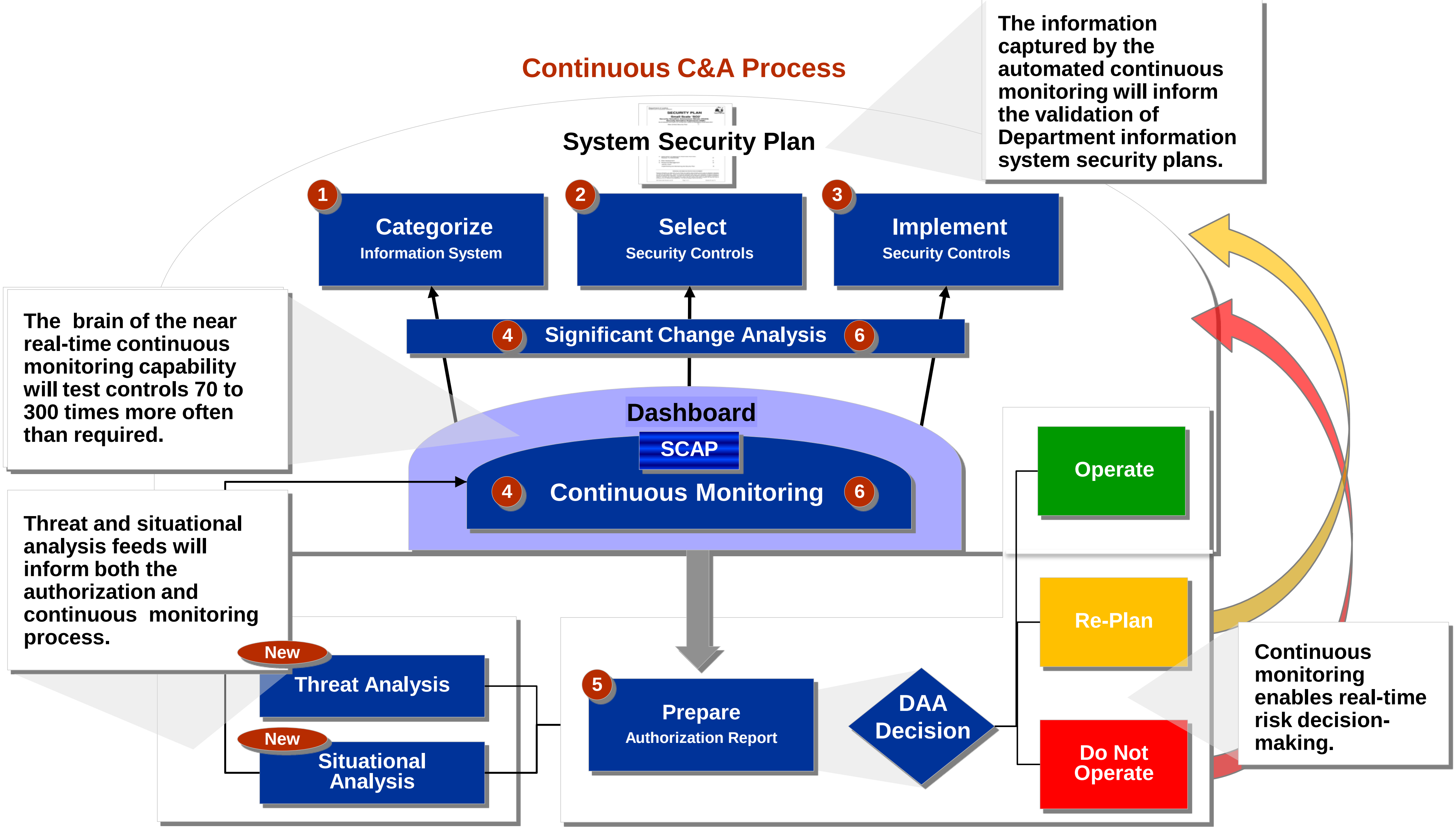
# = NIST 800-37 Rev. 1 Steps

# = NIST 800-37 Rev. 0 Mapping to Rev. 1 Steps

How can we apply the NIST steps to

- Fully comply with NIST rules, and
- Achieve decision-making based on near real-time monitoring?

The Department's continuous C&A process adheres to NIST rules and achieves near real-time monitoring



Continuous C&A Process
System Security Plan
1 Categorize Information System
2 Select Security Controls
3 Implement Security Controls
4 Significant Change Analysis 6
Dashboard
SCAP
4 Continuous Monitoring 6
New Threat Analysis
New Situational Analysis
5 Prepare Authorization Report
DAA Decision
Operate
Re-Plan
Do Not Operate

The information captured by the automated continuous monitoring will inform the validation of Department information system security plans.

The brain of the near real-time continuous monitoring capability will test controls 70 to 300 times more often than required.

Threat and situational analysis feeds will inform both the authorization and continuous monitoring process.

Continuous monitoring enables real-time risk decision-making.

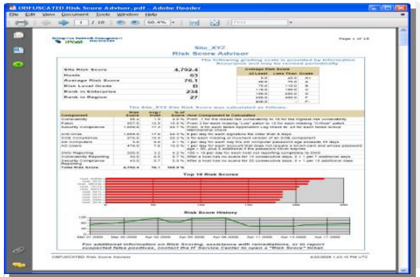
The continuous monitoring dashboard is the brain of near real-time C&A

Continuous Monitoring Process

NIST's steps 4 and 6 are really both about testing.

- Step 4 involves testing during "certification" and
- Step 6 involves testing during "monitoring"

These are really the same.



OBFUSCATED Risk Score Advisor.pdf - Adobe Reader

Site_XYZ

Risk Score Advisor

Site Risk Score	4,792.4
Hosts	63
Average Risk Score	76.1
Risk Level Grade	B
Rank in Enterprise	234
Rank in Region	27

The Site_XYZ Site Risk Score was calculated as follows:

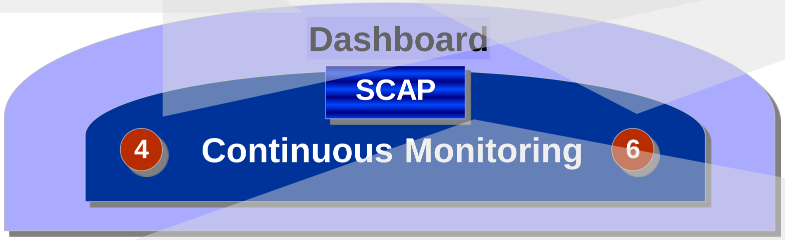
Top 10 Risk Scores

Risk Score History

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

OBFUSCATED Risk Score Advisor

The dashboard can (eventually) provide documentation of testing of all controls in a way that is timely, targeted, and prioritized.



The SCAP language, provided by NSA, NIST, etc., should be used as the way for testing tools to communicate results to the dashboard. This provides many benefits including:

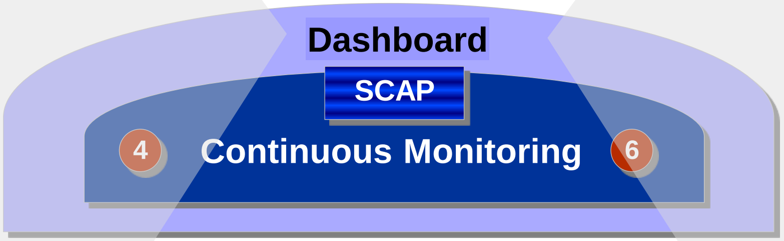
- Standardized language for conducting repeatable tests, and expressing test results in a re-usable format.
- Standardized re-usable content that can be borrowed from other agencies.
- Enabled comparison of test results for measurement and risk management.

The continuous monitoring dashboard offers both costs and benefits

Benefits

- **Operational managers know what high risk items need most to be fixed, and can easily find them.**
- **Senior managers have an easily understood measure of whether security is adequate.**
- **Risk is assessed 100-300 times more frequently than with traditional FISMA methods.**
- **Using SCAP allows easy communication of controls to sensors, and results to the dashboard.**
- **Demonstrated potential for 90% reductions in risk in 12 months.**

Continuous Monitoring Process



Dashboard

SCAP

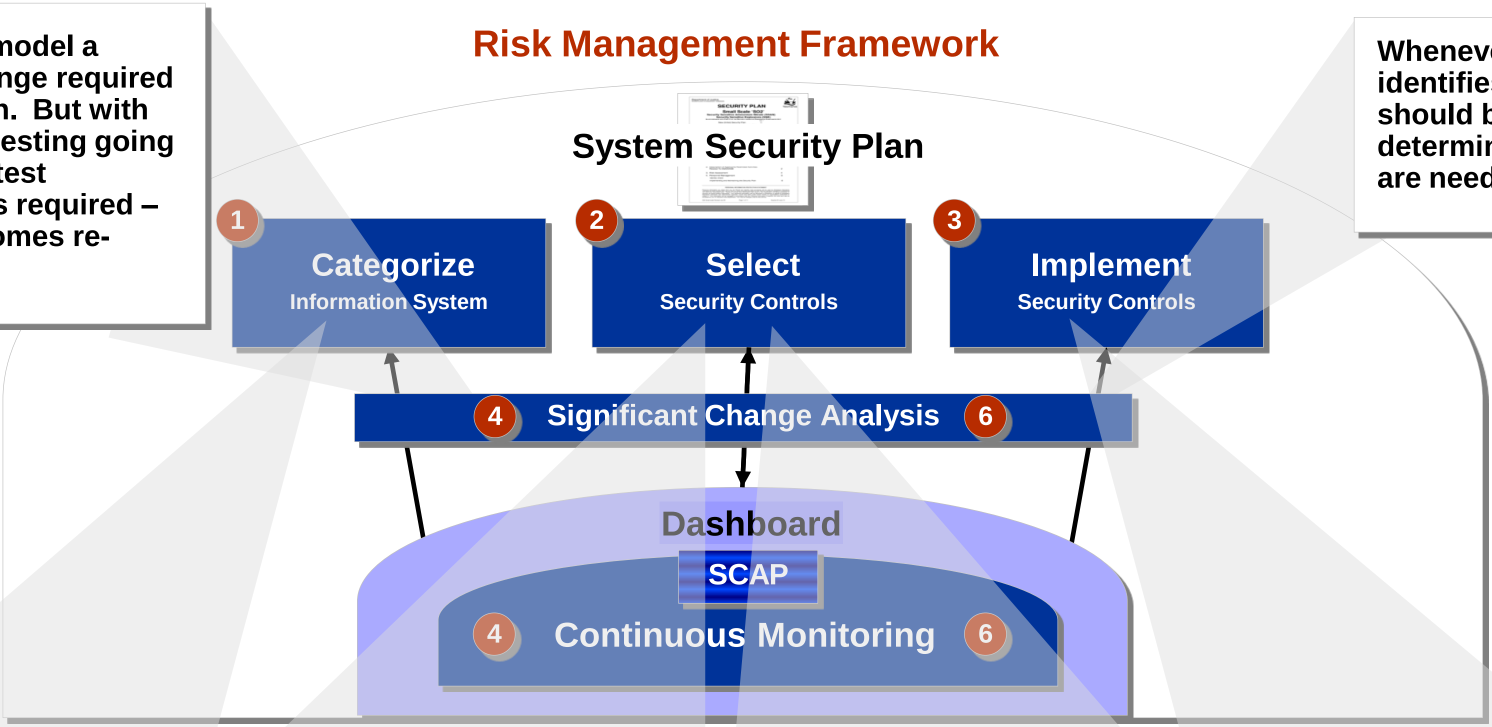
4 Continuous Monitoring 6

Costs

- **Initial phases can often use data from existing sensors to achieve major reductions in risk at low cost.**
- **Where new dashboard/sensors are needed they can be funded with what would have been spent on one-time tests for C&A.**
- **Effort to express controls in SCAP. (This can be reduced by reusing SCAP from the NIST/NSA library.)**
- **Communications, and business change management are needed to achieve full impacts.**

The dashboard dynamically feeds the Risk Management Framework

Under the old model a significant change required a recertification. But with near real-time testing going on, no special test (certification) is required – The focus becomes re-planning.



Whenever the dashboard identifies issues, they should be evaluated to determine whether changes are needed to the SSP.

When the dashboard identifies new kinds of sensitive data in a system, that can immediately trigger re-categorization.

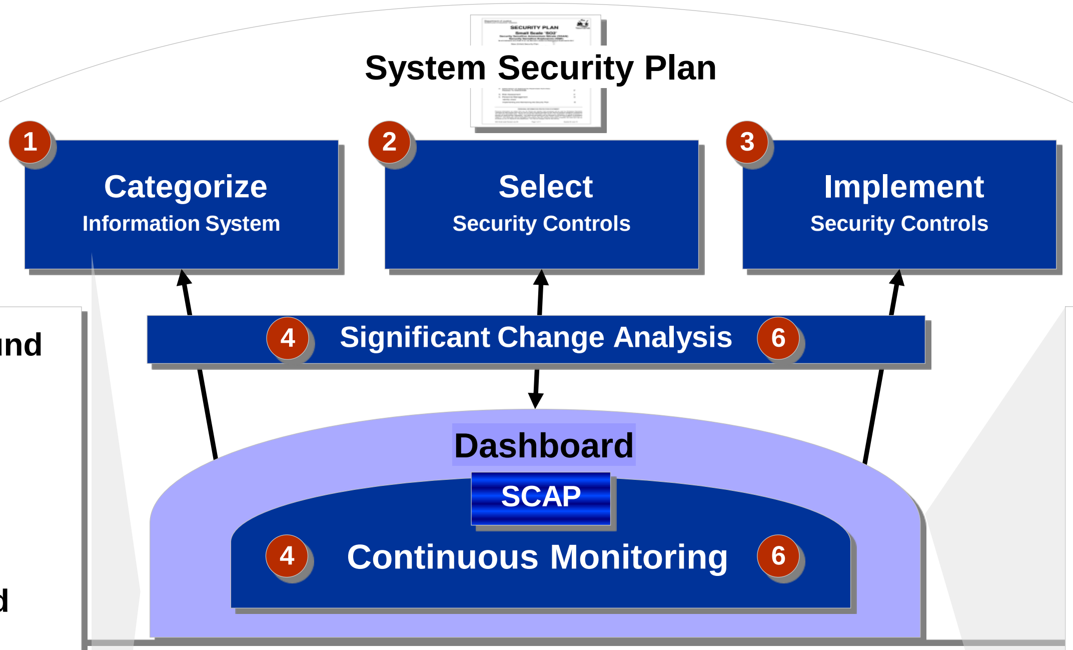
When the dashboard identifies new components (e.g., data base links not in the SSP) it can be used to trigger human authorization and SSP update, if appropriate.

The Security Plan informs the dashboard of what controls needs to be tested (These need to be recorded as SCAP tests).

When the dashboard identifies controls that need attention, it informs operators to change the implementation to make the controls work.

The system security process offers both costs and benefits

System Security Process



Benefits

- Control problems are found and fixed faster.
- The most significant problems are addressed first.
- Unplanned/Unannounced changes to data and controls are found sooner.
- If the security controls are expressed in SCAP, rather than text, then automation can be accelerated.

Costs

- There is little additional cost beyond what was described earlier.
- Communications, training, and business change management are key.

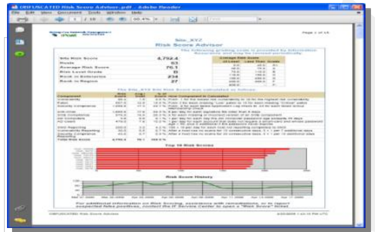
Because of "continuous" testing, we can have "continuous" authorization

Continuous Authorization Process

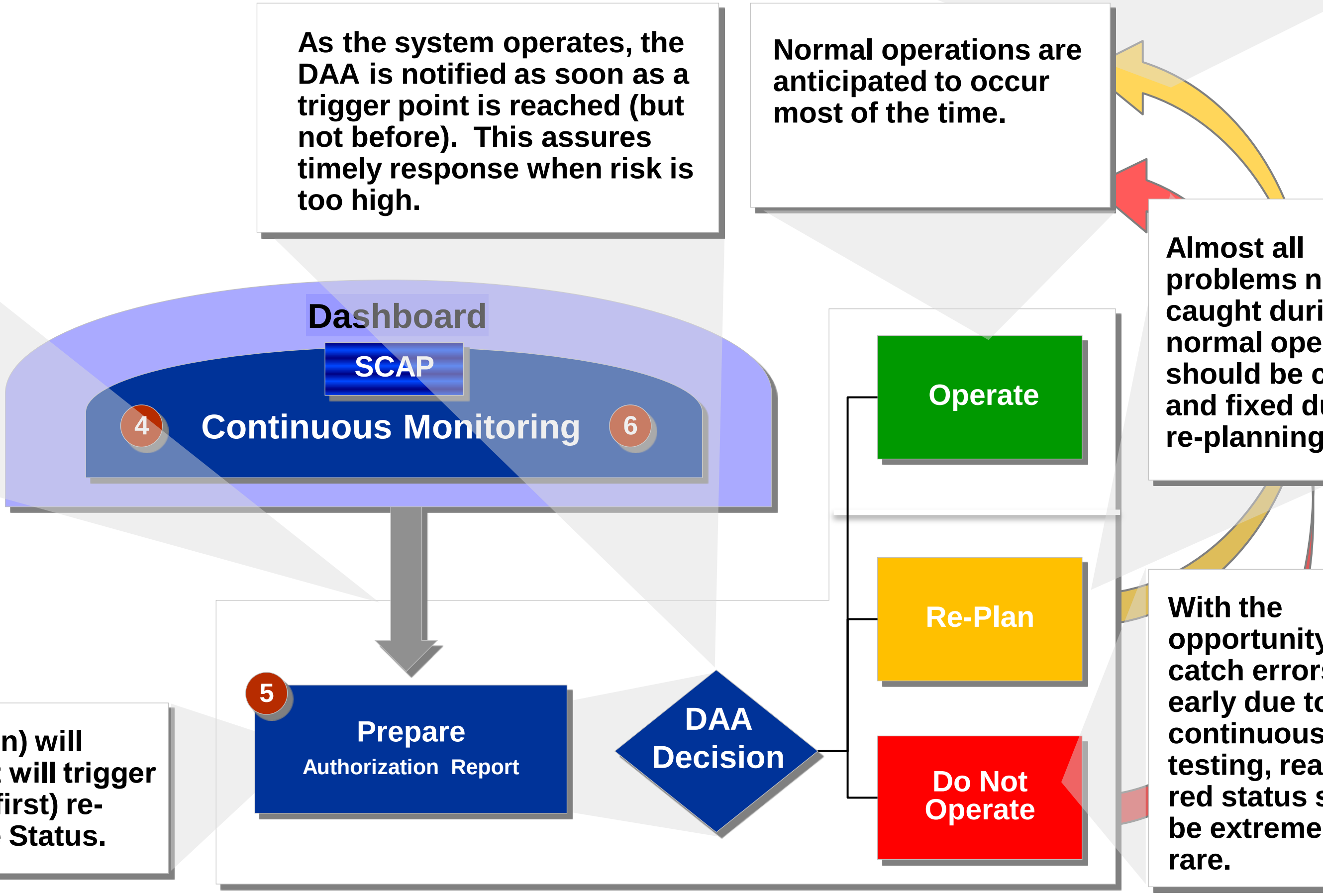
Whenever the dashboard identifies issues, they should be evaluated to determine whether changes are needed to the SSP

As the system operates, the DAA is notified as soon as a trigger point is reached (but not before). This assures timely response when risk is too high.

Normal operations are anticipated to occur most of the time.



The Dashboard provides a "risk score" for each system.



Almost all problems not caught during normal operations, should be caught and fixed during re-planning.

The DAA (as part of initial authorization) will define "trigger points" (risk levels that will trigger a change from normal operations, to (first) re-planning and (second) Do not Operate Status.

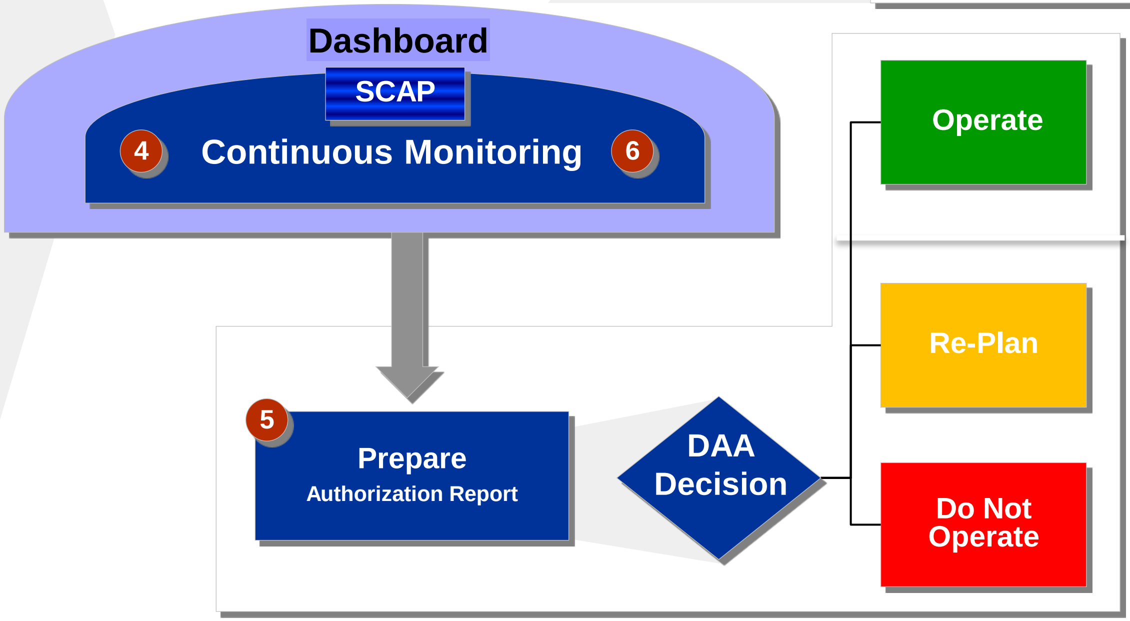
With the opportunity to catch errors early due to continuous testing, reaching red status should be extremely rare.

The continuous authorization process offers both costs and benefits

Benefits

- DAA rests assured that risk is being monitored frequently, and that they will be alerted if a trigger point is reached.
- When a trigger point is reached, the DAA has a tangible and understandable risk measure (grade, rank, and score).
- Most risks will be fixed before yellow is ever reached.
- The yellow alert level provides time to fix essentially all remaining risks before red status is reached.

Continuous Authorization Process

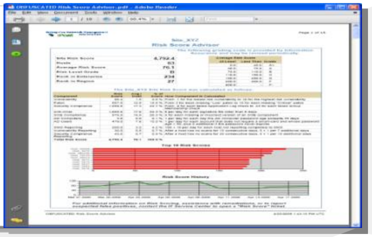


Costs

- Cost for DAA reviews should be reduced because of better summarization.
- Costs of testing and remediation become incidental daily expenses, rather than major periodic expenses.

The new NIST risk framework emphasizes a focus on all levels of risk – which adds a new dimension to C&A

The threat and situational analysis will send risk scoring adjustments to the dashboard to enable system owners to focus on the highest risks first



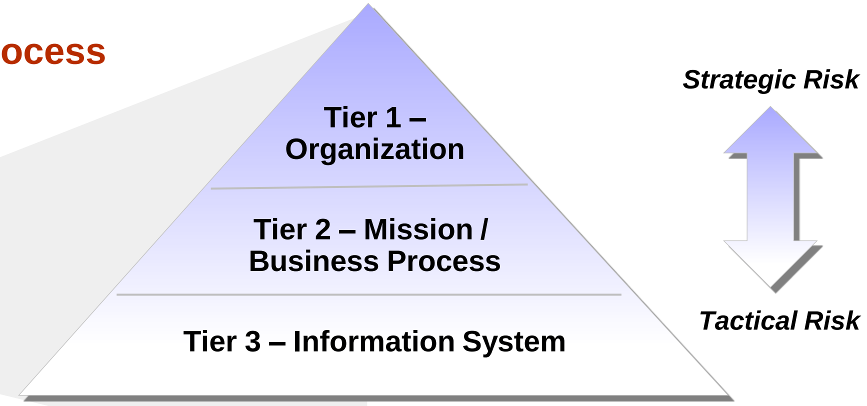
OBFUSCATED Risk Score Advisor.pdf - Adobe Reader

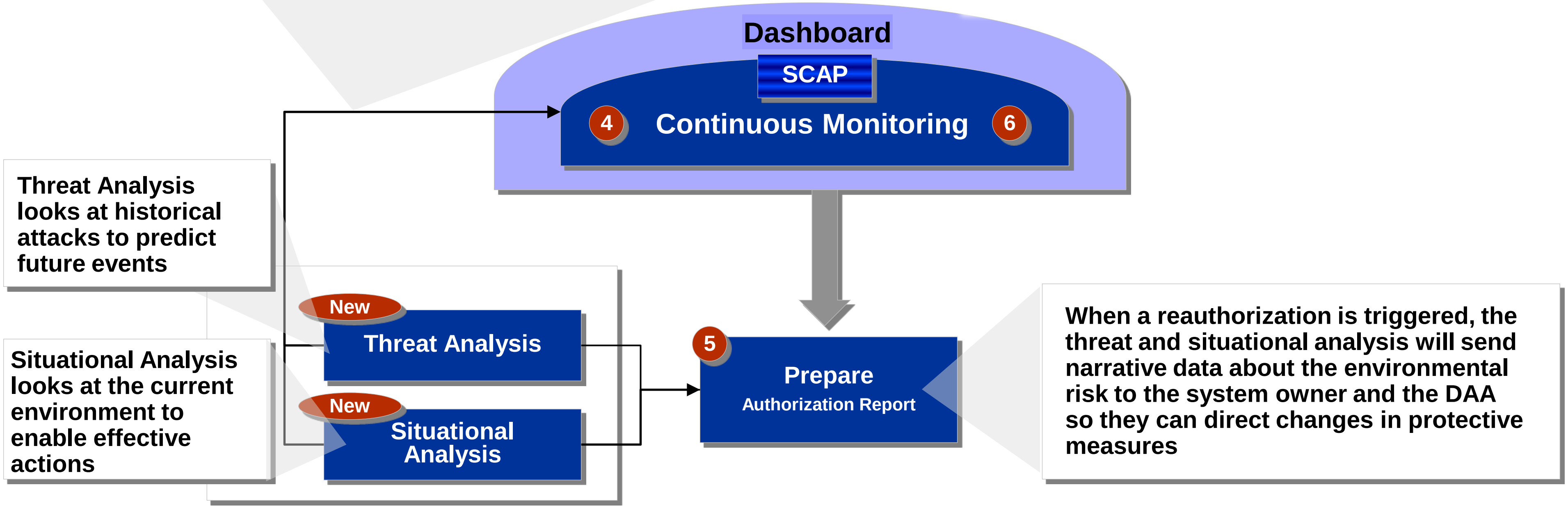
Site_XYZ
Risk Score Advisor

Site Risk Score	4,792.4
Hosts	63
Average Risk Score	76.1
Risk Level Grade	B
Rank in Enterprise	234
Rank in Region	27

Top 10 Risk Scores

Risk Score History





Threat Analysis looks at historical attacks to predict future events

Situational Analysis looks at the current environment to enable effective actions

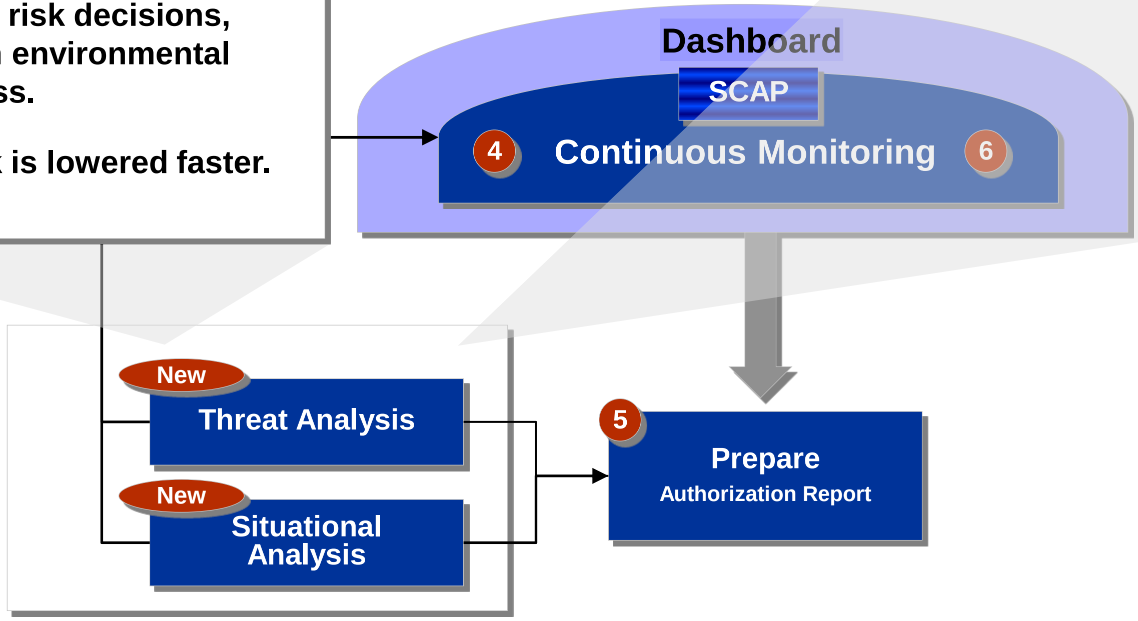
When a reauthorization is triggered, the threat and situational analysis will send narrative data about the environmental risk to the system owner and the DAA so they can direct changes in protective measures

The enterprise risk process offers both costs and benefits

Benefits

- These inputs fine tune risk scores to ensure rapid attention to real threats by operational managers.
- This is a major workforce multiplier.
- The narrative provided to the DAA enables more informed risk decisions, based on environmental awareness.
- Total risk is lowered faster.

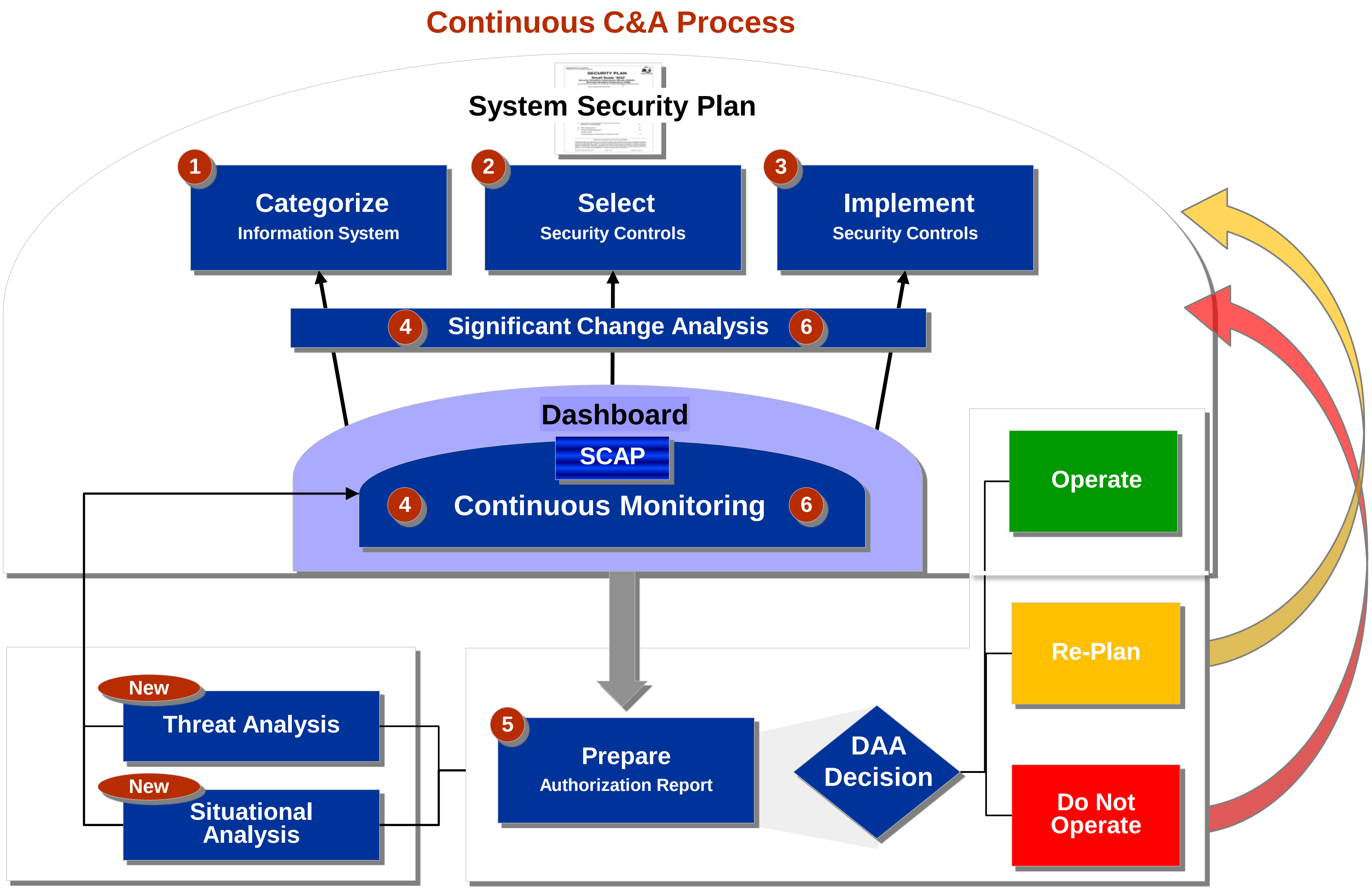
Enterprise Risk Process



Costs

- Additional tools are needed for these analyses, if not already in place.
- These tools also be funded from what would have been spent on one-time C&A studies.
- The cost of analysis is small compared to the leveraged impact it has on operational security.

Continuous C&A Process will provide more effective real-time security – not just a snapshot in time

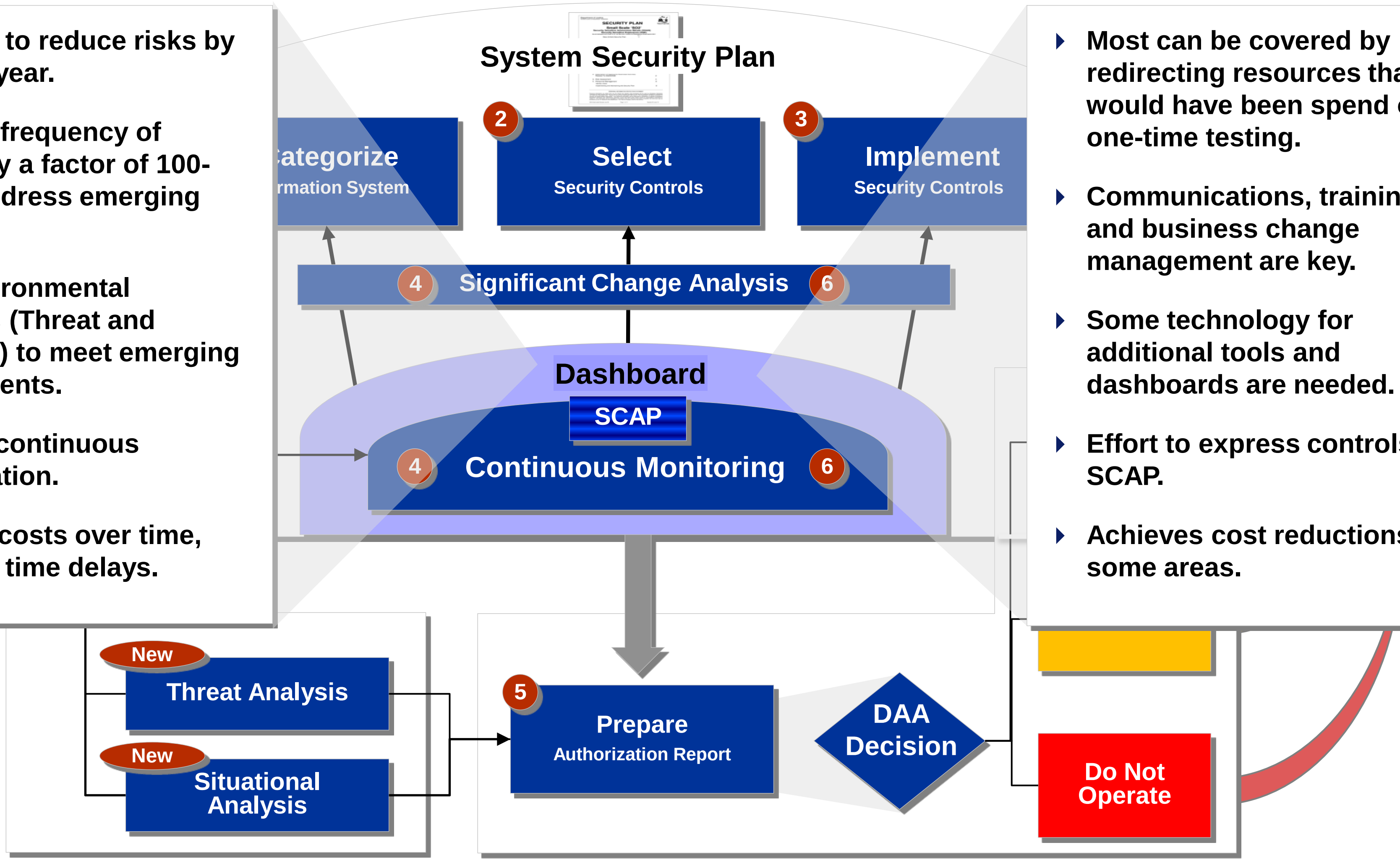

Continuous C&A Process
System Security Plan
1 Categorize Information System
2 Select Security Controls
3 Implement Security Controls
4 Significant Change Analysis 6
Dashboard
SCAP
4 Continuous Monitoring 6
New Threat Analysis
New Situational Analysis
5 Prepare Authorization Report
DAA Decision
Operate
Re-Plan
Do Not Operate

Although there is some cost inherent in the Continuous C&A process, its benefits are significant – and cannot be ignored

Benefits

- Potential to reduce risks by 90% per year.
- Increase frequency of testing by a factor of 100-300 to address emerging threats.
- Add Environmental Analyses (Threat and Situation) to meet emerging requirements.
- Enables continuous accreditation.
- Spreads costs over time, reducing time delays.

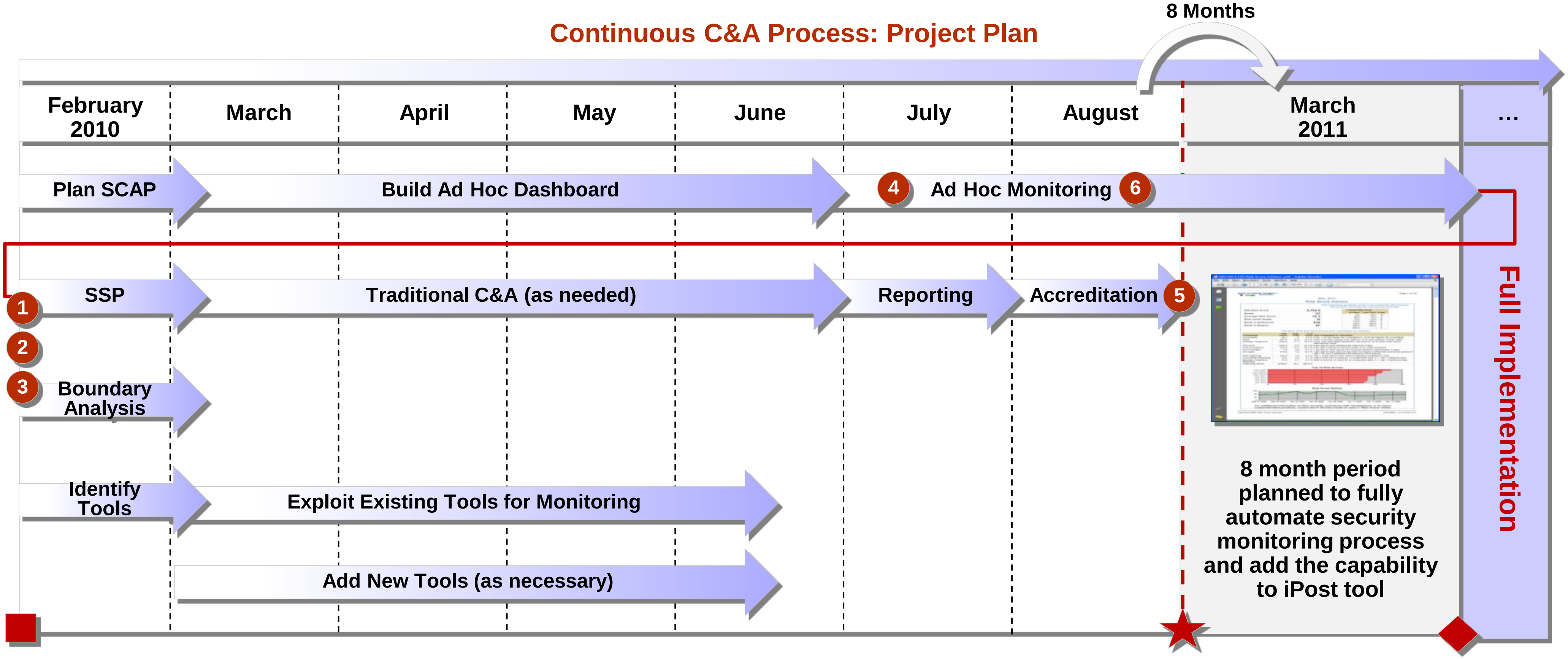
Continuous C&A Process



Costs

- Most can be covered by redirecting resources that would have been spend on one-time testing.
- Communications, training, and business change management are key.
- Some technology for additional tools and dashboards are needed.
- Effort to express controls in SCAP.
- Achieves cost reductions in some areas.

The pilot of the Continuous C&A process on OpenNet and ClassNet will be completed by August 31st



Continuous C&A Process: Project Plan

8 month period planned to fully automate security monitoring process and add the capability to iPost tool

February 1st 2010

August 31st 2010

March 31st 2011

All of the required six steps from NIST SP 800-37 Rev. 1 are covered in this Continuous C&A Process

For further information on the Department of State's Continuous C&A Strategy, please reach to the following POCs

Points of Contact

John Streufert
Chief Information Security Officer

Department of State, IRM/IA
Arlington, VA 22209
Tel (703) 812-2555
streufertj@state.gov

George Moore
Chief Computer Scientist

Department of State, IRM/IA
Arlington, VA 22209
Tel (703) 812-2203
mooregc@state.gov

Pete Gouldmann
NIST & CNSS Liaison

Department of State, IRM/IA
Arlington, VA 22209
Tel (703) 812-2201
gouldmannp@state.gov

Sara Mosley
Senior Security Engineer

Department of State, IRM/IA
Arlington, VA 22209
Tel (703) 812-2555
mosleysn@state.gov